Appl. No. 10/634,881
Reply to Office Action of: December 12, 2006

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of distributing certificates to a plurality of mobile devices ~~by establishing a mobile ad hock network (MANET) between a plurality of mobile devices at a predetermined time and distributing a certificate through said mobile ad hoc network to a respective one of said mobile devices.~~ capable of communicating directly with each other comprising:
- attempting to establish a mobile ad hoc network (MANET) between said plurality of mobile devices at periodic predetermined times; and
- if said MANET can be established such that at least one of said plurality of mobile devices in said MANET is capable of obtaining certificates, distributing a certificate through said MANET to one or more of said plurality of mobile devices.

2. (currently amended) The method of claim 1 wherein ~~the times~~ a time period for which [[a]] said certificate is valid is correlated to [[the]] said periodic predetermined time~~s for establishing said MANET~~.

3. (currently amended) The method of claim 1 wherein if [[a]] one of said plurality of mobile devices [[that]] is unable to retrieve [[its]] a corresponding certificate within a preset time after ~~the establishment of a~~ said MANET is established, said one of said plurality of mobile devices subsequently attempts to participate in another ad-hoc ~~networks~~ network prior to [[the]] a next predetermined time to retrieve [[its]] said corresponding certificate.

4. (currently amended) The method of claim 1 wherein if [[a]] one of said plurality of mobile devices [[that]] is unable to retrieve [[its]] a corresponding certificate within ~~an amount of~~ a present time after [[the]] said MANET ~~establishment~~ is established, said one of said plurality of mobile devices initiates a ~~cellular~~ packet data call to ~~fetch its~~ obtain said corresponding

Best Available Copy

certificate.

5. (currently amended) The method of claim 1 wherein an entity tracks which of said plurality of mobile devices have received currently valid certificates.

6. (currently amended) The method of claim 5 wherein [[a]] corresponding certificates of [[a]] said plurality of mobile devices which [[has]] have not received an up-to-date certificate [[is]] are distributed to another one of said plurality of mobile devices that communicates with said entity.

7. (currently amended) The method of claim 1 wherein [[the]] said predetermined times for establishing the MANET is are determined dynamically based upon measurements of times at which said plurality of mobile devices encounter each other.

8. (currently amended) The method of claim 1 wherein the information in said distributed certificate comprises a subset of [[the]] full certificate information and [[the]] said subset includes changed timing information and a signature.

9. (currently amended) A method of distributing certificates in a mobile ad-hoc network (MANET), said MANET having an access point to provide a connection for connecting to a communication network and comprising a plurality of mobile devices to be connected to said communication network through said access point, said method comprising the steps of
_retrieving and storing at said access point, a plurality of certificates associated with respective ones of said plurality of mobile devices;
- storing said plurality of certificates at said access point; and
- upon establishing said MANET, forwarding said certificates through said mobile ad-hoc network MANET to said respective ones of said plurality of mobile devices.

10. (currently amended) The method of claim 9 wherein said access point queries those of said plurality of mobile devices with which it can exchange packets to determine [[their]] an embedded root key.

3

11. (currently amended) The method of claim 10 wherein the access point ~~fetches~~ obtains said plurality of certificates based upon said embedded root [[keys]] key.

12. (currently amended) A method of distributing certificates within a mobile ad-hoc network (MANET) of a plurality of mobile devices comprising ~~wherein~~ having an online entity associated with ~~a device is~~ at least one of said plurality of mobile devices be responsible for both distributing ~~the device's~~ a certificate of said at least one of said plurality of mobile devices within said MANET and for ~~fetching~~ obtaining other certificates needed to allow validation by ~~another device~~ corresponding others of said plurality of mobile devices in said ~~network~~ MANET.

13. (currently amended) The method of claim 12 wherein said at least one of said plurality of devices is responsible for collecting embedded root keys of said others of said plurality of devices ~~with which it comes in~~ upon coming into contact therewith.

14. (original) The method of claim 13 wherein said root keys are reported to the online entity.

15. (currently amended) The method of claim 14 wherein said online entity returns other certificates to [[the]] said at least one of said plurality of devices based upon [[the]] reported root keys.

16. (currently amended) A method of securely setting a time source in a first mobile device ~~from~~ capable of communicating with a second mobile device, said method comprising said first mobile device ~~the steps of~~:
- establishing a shared secret ~~between the two devices~~ with said second device using certificates;
- storing [[the]] said shared secret in a non-volatile memory;
- ~~a first of said devices~~ authenticating [[a]] said second ~~of said devices~~ device using [[the]] said shared secret; and
- obtaining ~~transferring the~~ a time from [[the]] said second device to ~~the first device~~ enable said time source to be set.

Best Available Copy

17. (currently amended) The method of claim 16 wherein [[the]] said shared secret is destroyed after an expiration time.

18. (currently amended) The method of claim 16 wherein [[the]] said first device subsequently sets [[its]] a clock via a secure time source when it subsequently can upon establishing a connection thereto.

19. (currently amended) A method of a first mobile device validating a second mobile device, wherein said first and second mobile devices are capable of communicating with each other, said method comprising:
- said first mobile device obtaining wherein a certificate presented to a first device by a from said second device;
- said first mobile device determining if said certificate has expired;
- if said certificate has not expired, said first mobile device using said certificate to validate said second mobile device; and is used for the validation if the second device's certificate has not expired
- if said certificate has expired, said first mobile device obtaining another certificate for said second mobile device using a pointer provided by said second mobile device and validating said second mobile device using said another certificate. and wherein the fist device uses for the validation a certificate fetched based upon a pointer presented by the second device if the second device's certificate has expired

20. (currently amended) A method of distributing certificates wherein when a first mobile device cannot is unable to retrieve a certificate at a first time because there is no due to a lack of connectivity to the internet a network, said method comprising the steps of:
- if said certificate has not been obtained by a second time, said first mobile device requesting assistance of other devices if the certificate has still not been received by a second time;
- having a second device of the from said other devices which has connectivity to said network request [[the]] said certificate on behalf of [[the]] said first device when the second device has connectivity to the internet;
- upon obtaining said certificate, having the said second device reestablishing communication

5

with [[the]] said first device; and

- said second device sending [[the]] said certificate from the second device to [[the]] said first device.

6